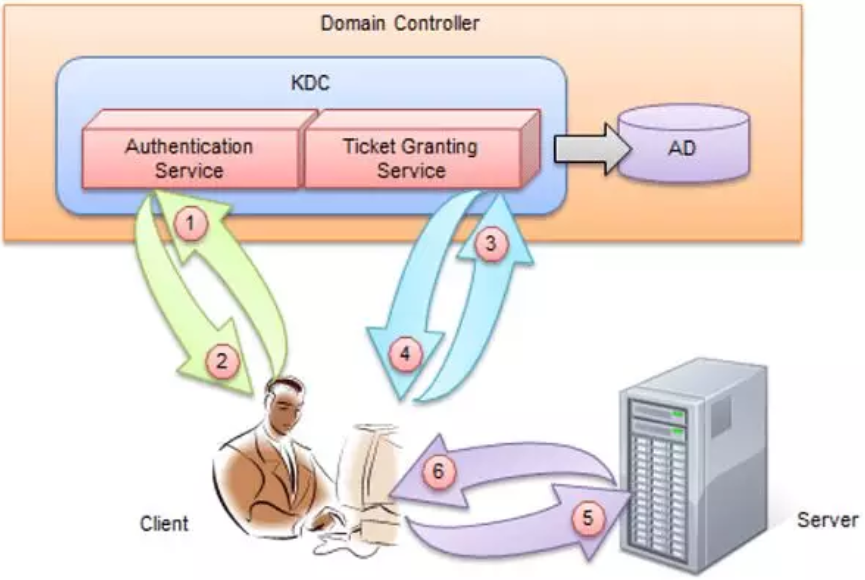
**Kerberoasting后门(随时破解ST获取服务账户密码):**



服务主体名称(Service Principal Names SPN)是服务器运行服务的唯一标识，每个使用kerberos协议的服务都需要注册一个SPN,SPN分为两种，一种注册在域内机器用户账户(Computer),一种注册在域内用户账户(User)。机器账户一般是默认注册的，如果在域用户下运行服务，必须手动注册SPN,用到setspn.exe。

SYSVOL存在于域中的所有域控中。包含公共文件的共享文件夹，包括组策略数据 ，经过认证的用户都可以访问该文件夹。所有域组策略都存储在这里：\\ <DOMAIN> \ SYSVOL \ <DOMAIN> \ Policies \

在win2k8中添加了GPP选项，即组策略首选项，可以完成更多的系统及应用管理，比如说管理本地用户 添加计划任务等。

在08的域控上为域主机远程添加用户，所有的操作都会写到Group.xml文件中，包括创建的账户名称 时间 以及加密后的密码。该密码默认是用AES256加密的，而且官方提供了完整的密钥,正好用来解密得到密码。漏洞的补丁编号为KB2962486.

为指定拥有高权限的域用户添加SPN，可随时请求到该域用户的ST，破解得账户密码明文

添加命令:

setspn.exe -U -A backdoor/dcs.threathunting.com Administrator

删除命令:

setspn.exe -D backdoor/dcs.threathunting.com Administrator

**域管权限维持:**

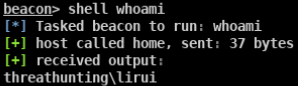
**SSP记录登录到当前机器的所有账号密码明文:**

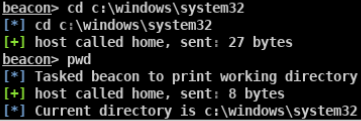
Security Support Provider是用于身份验证的dll，系统在启动时会将其加载到lsass.exe进程中，由于lsa可扩展，若在系统启动时加载一个自定义的恶意dll则达到恶意攻击目的。

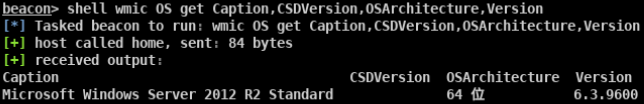
方式一(永久记录，重启有效):

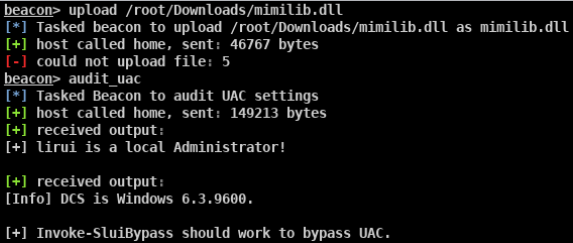
域管身份



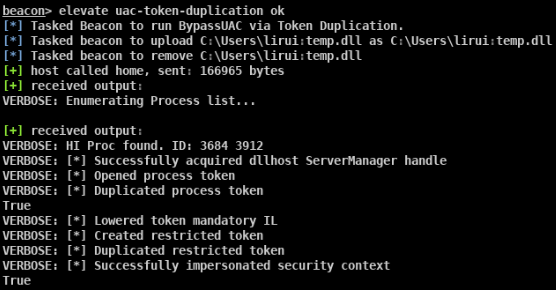




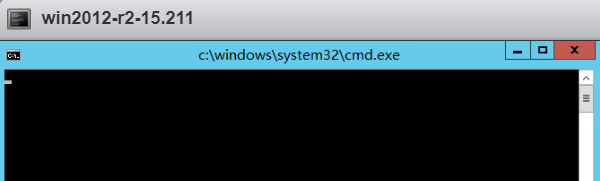




进行BypassUAC:

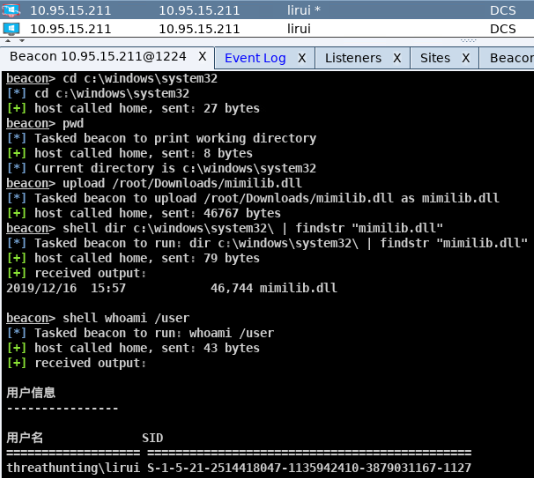


域控会弹出cmd窗口:

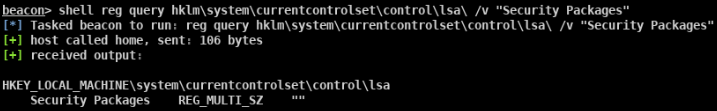


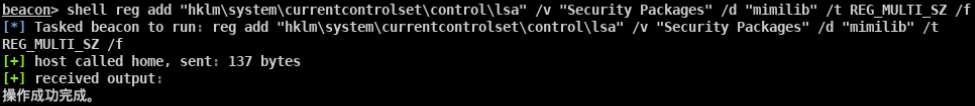


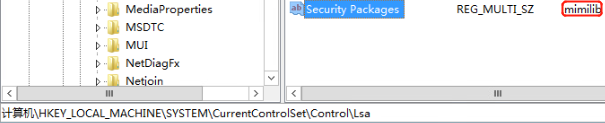
上传mimilib.dll:

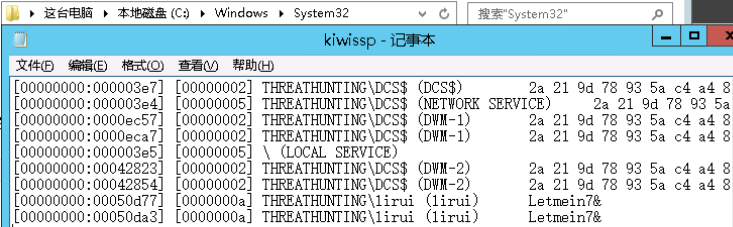


修改注册表:





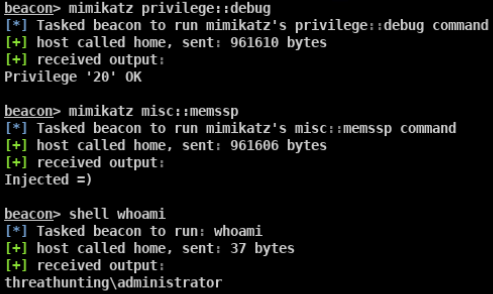


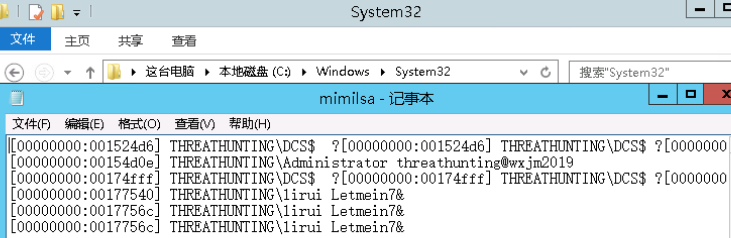


方式二(执行后生效，重启失效):

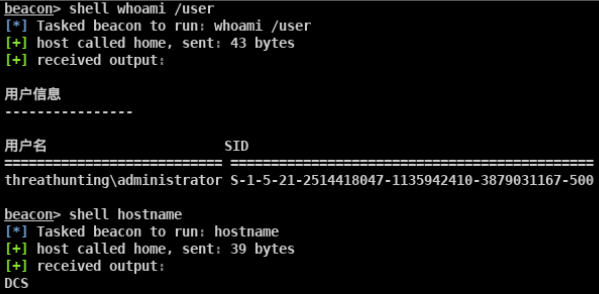
需使用域管administrator身份的shell

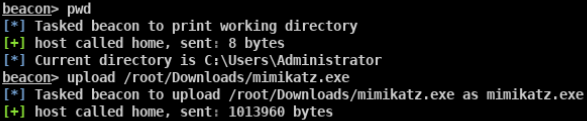


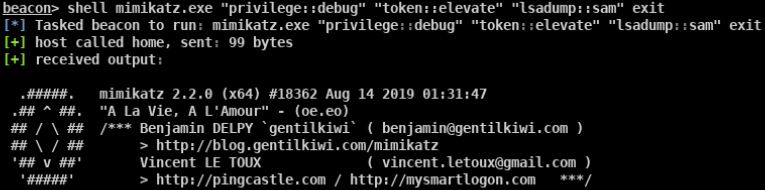




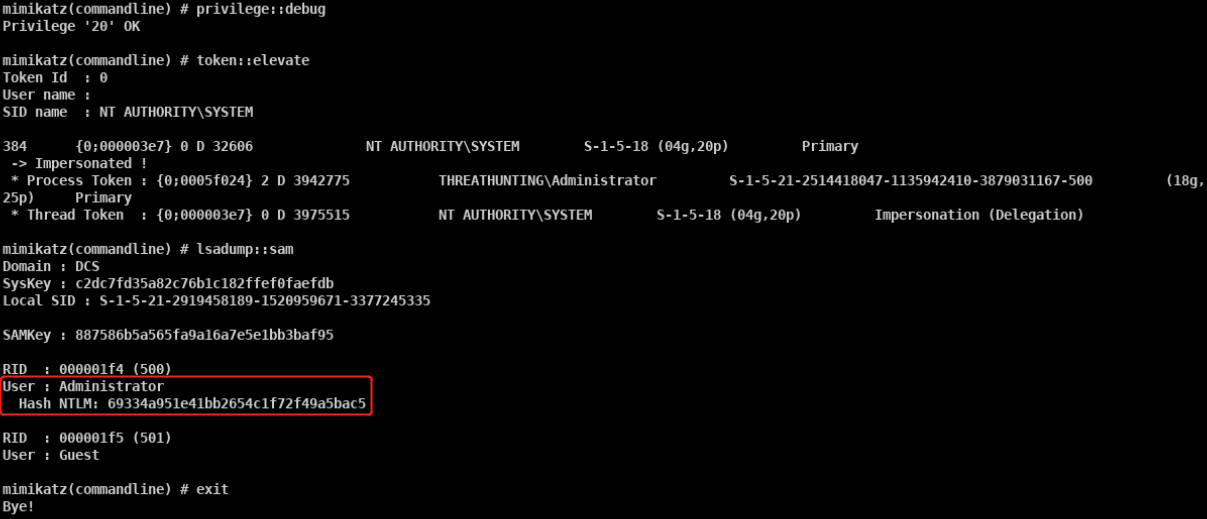
**DSRM账户同步域内任意账户密码(重启不失效):**

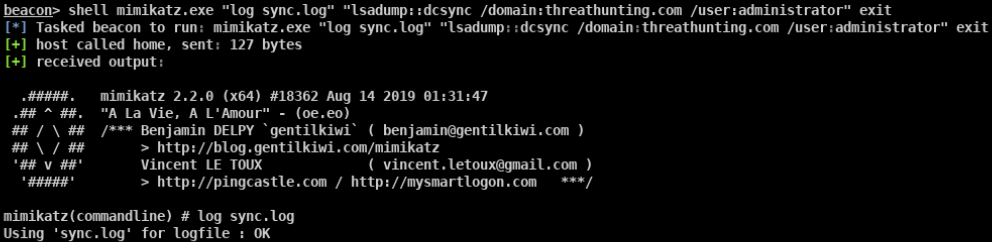




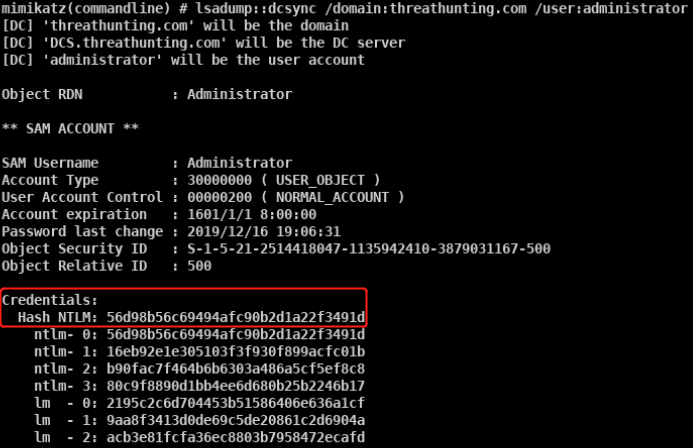


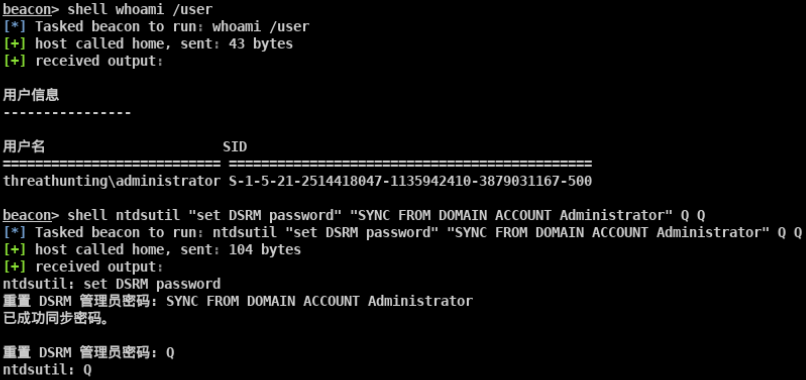
本地DSRM[administrator]账户Hash:



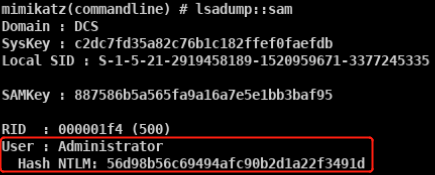


内建域管administrator密码hash:

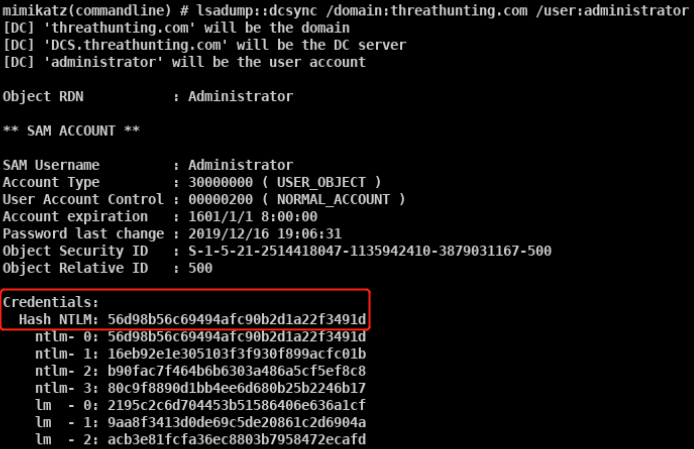










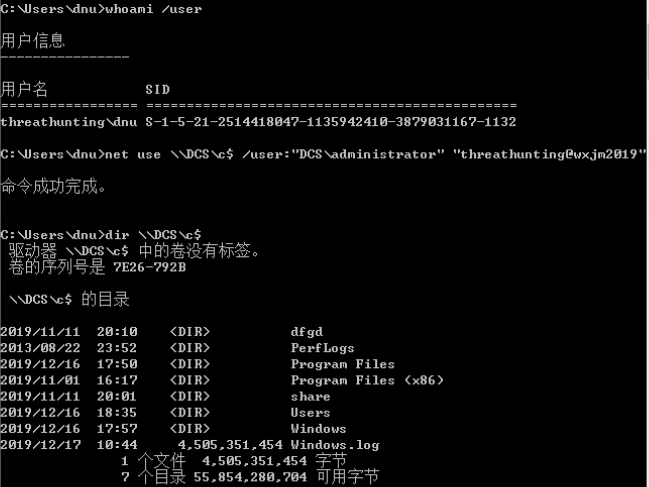


发现DSRM账户已经同步域管administrator账户的密码哈希

允许DSRM账户远程访问:

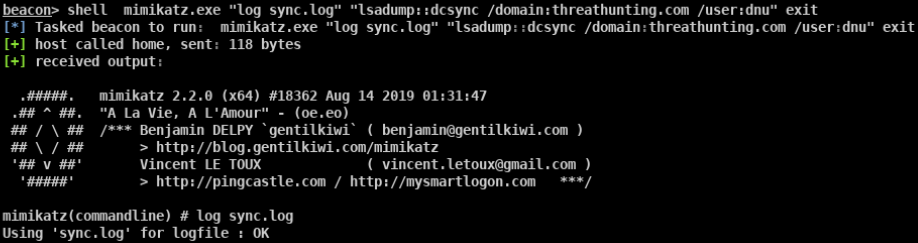


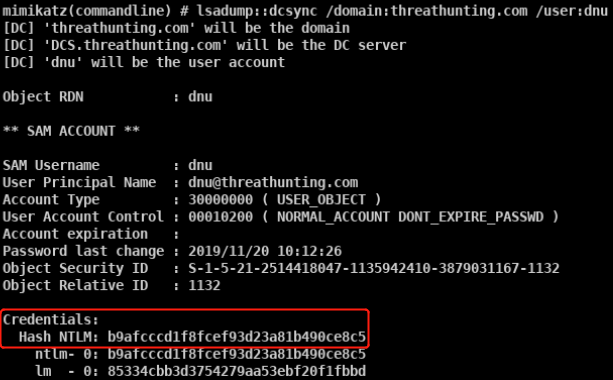
破解hash获得明文后连接域控:

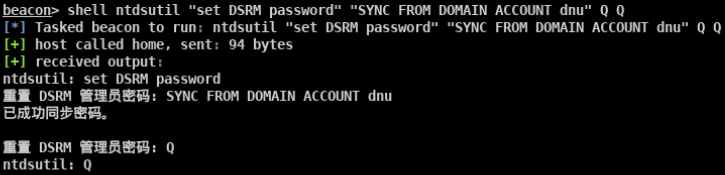


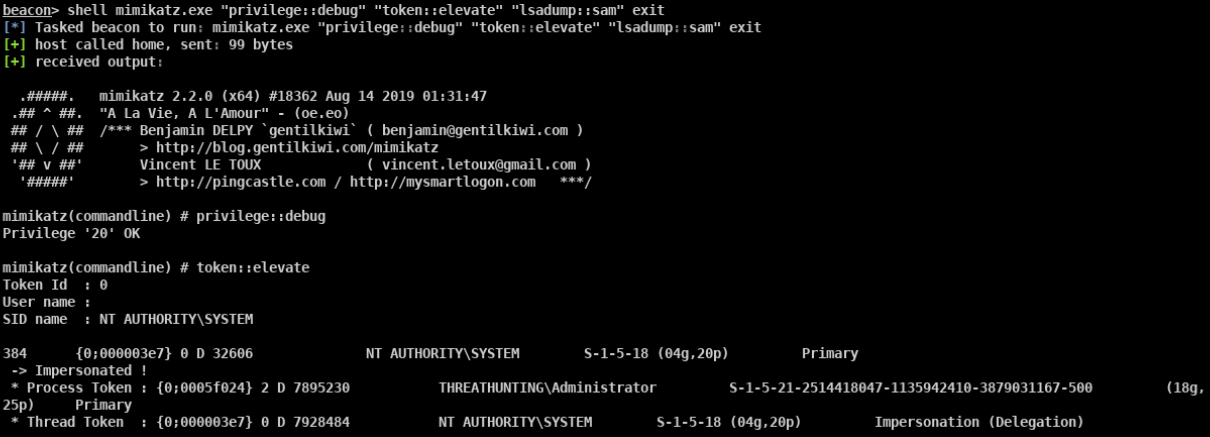
DSRM账户同步域内普通账户的密码哈希:

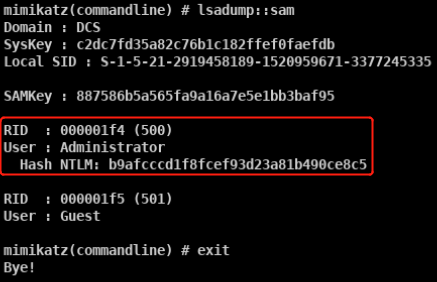




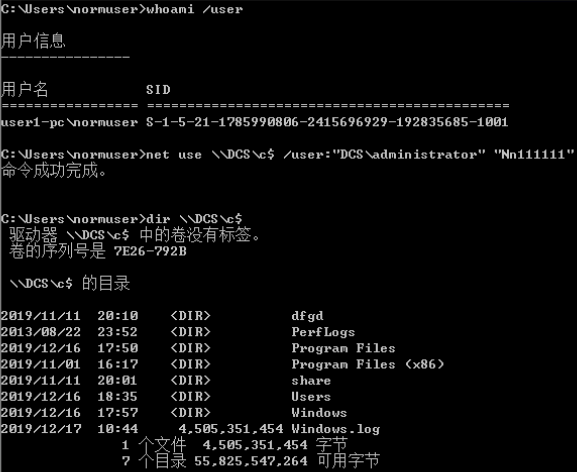








破解hash获得明文后连接域控:



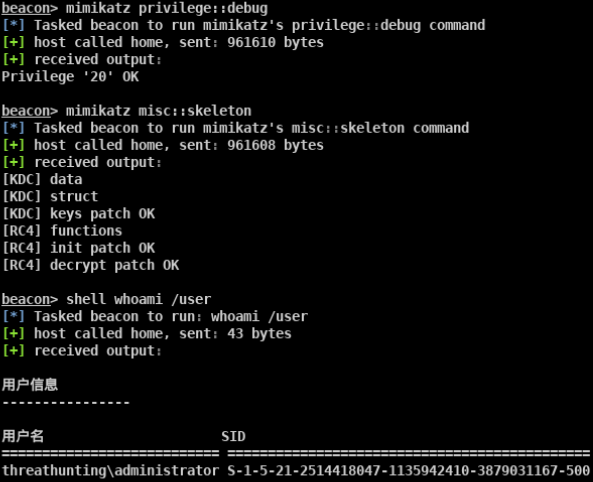
检测方法:

监测安全事件日志: id=4794 - 尝试设置目录服务还原模式管理员密码

**域控万能钥匙-Skeleton Key(可使域内任意用户使用同一密码登入域控，普通域用户可成功登陆，但不具有访问权限):**

适用于Windows Server2003—Windows Server2012 R2，本次实验使用2012 R2。

内置域管administrator身份执行:



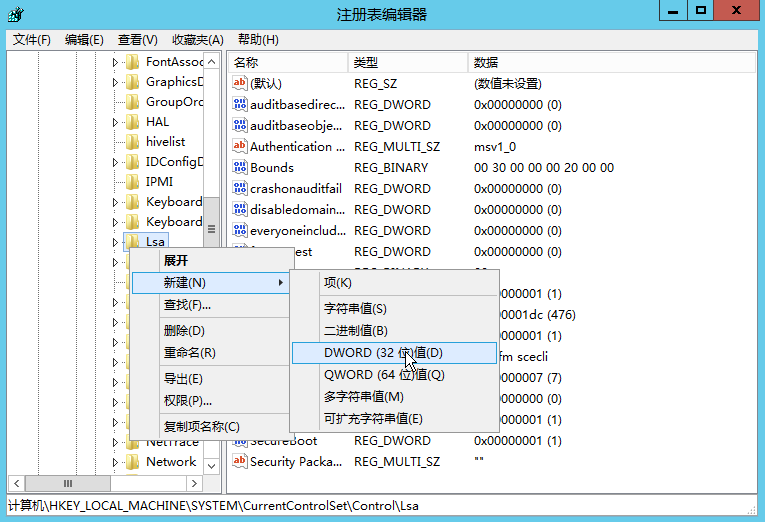


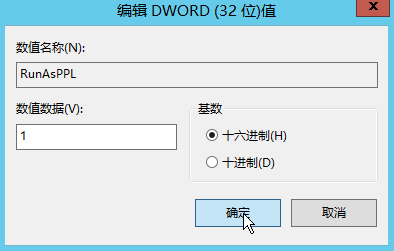
域控重启后失效:



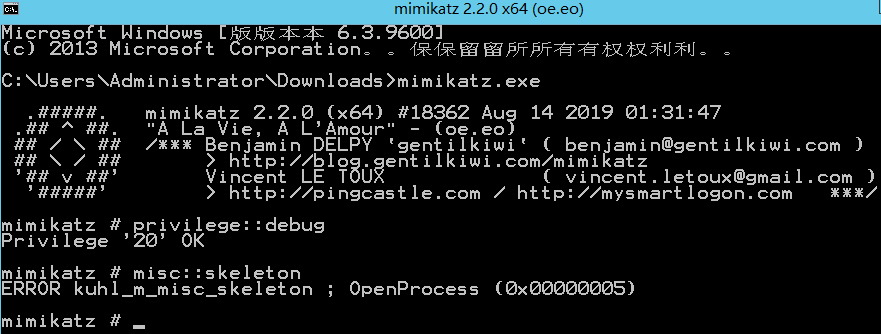
2014年微软添加了LSA保护策略:

启用LSA保护策略-防止对lsass.exe进程进行代码注入:

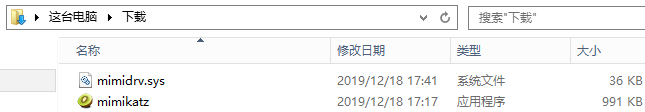


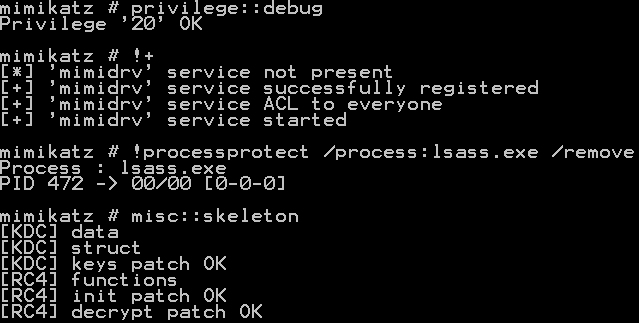


重启域控生效:



执行如下操作(通过mimidrv.sys驱动文件绕过LSA保护策略):







可在源码中修改万能密码为特定值:

https://github.com/gentilkiwi/mimikatz/blob/master/mimikatz/modules/kuhl\_m\_misc.c

**Hook PasswordChangeNotify函数隐形记录变更密码:**

正常修改域控密码的过程:

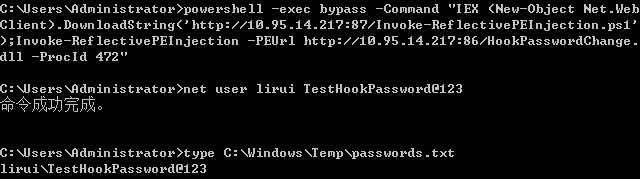
LSA 首先调用 PasswordFileter 判断新密码是否符合密码复杂度的要求，若符合 ,LSA会继续调用PasswordChangeNotify 在系统上同步更新的密码

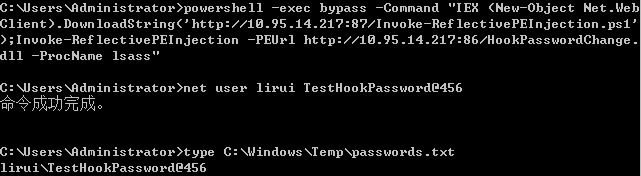
PasswordChangeNotify函数在rassfm.dll中(此dll只存在于Windows Server中)

进程注入(重启失效):

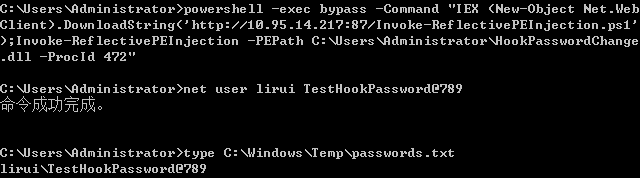
反射型dll注入hook PasswordChangeNotify函数秘密记录密码修改情况:



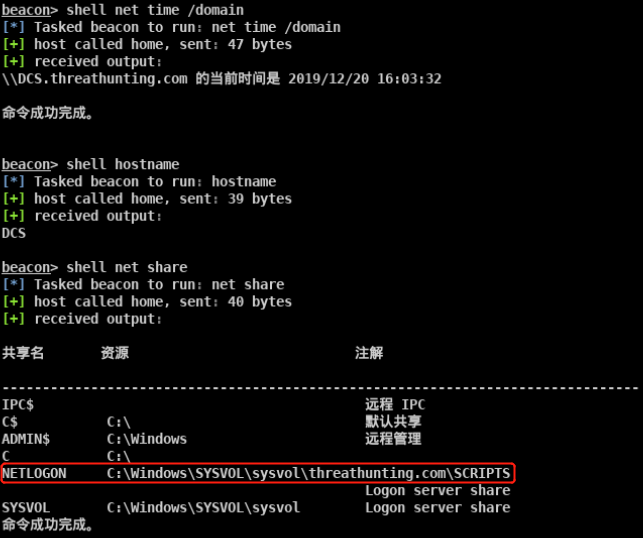


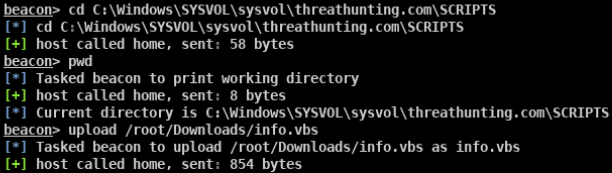


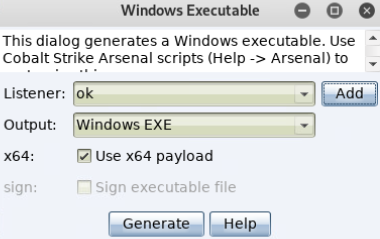
从本地加载恶意dll并注入到lsass进程:



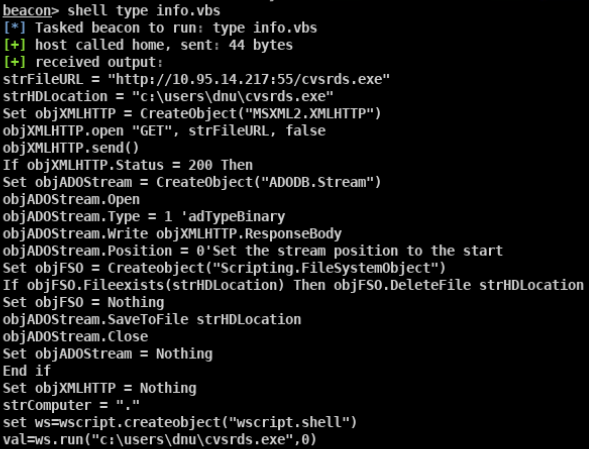
**针对特定域用户挂马:**

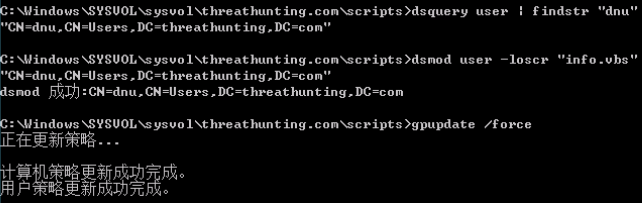




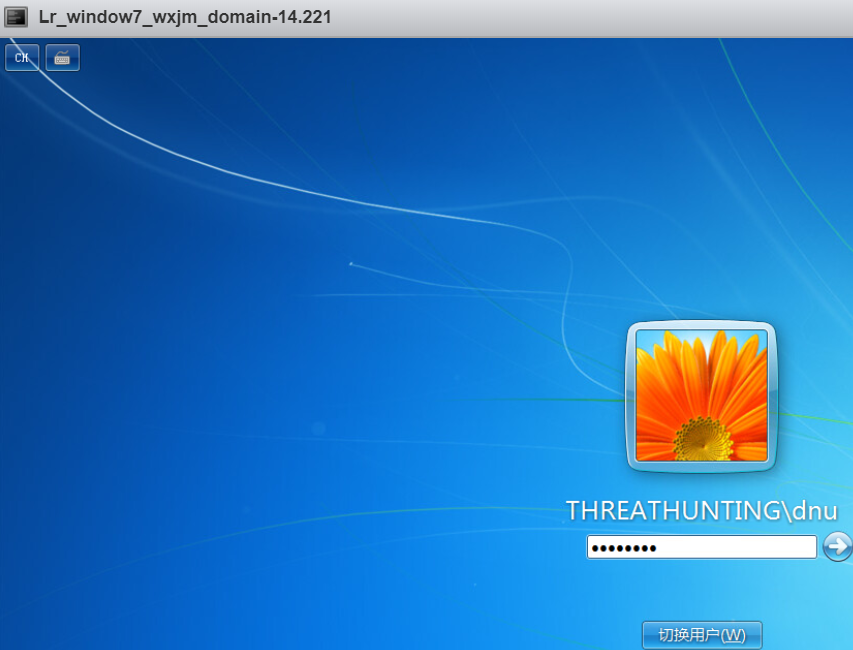














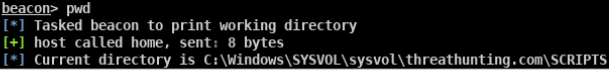
**批量挂马实现域内用户批量上线**:

info.vbs:

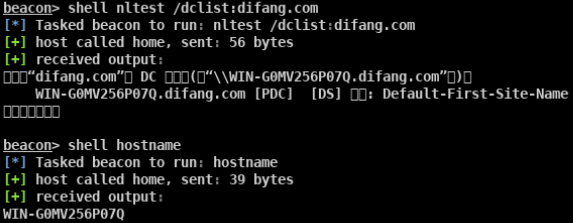


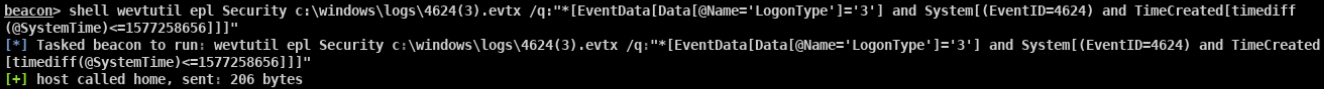


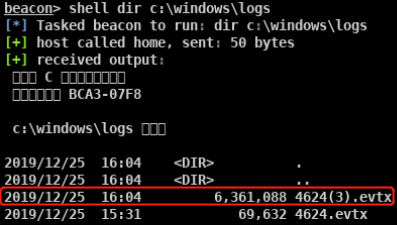
目标稳定上线后删除域控上的vbs脚本(所在目录如下图)即可:

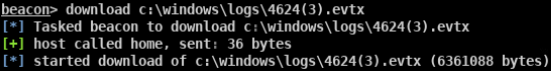


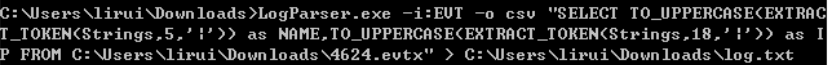
**指定域用户打击(域用户登录日志利用):**

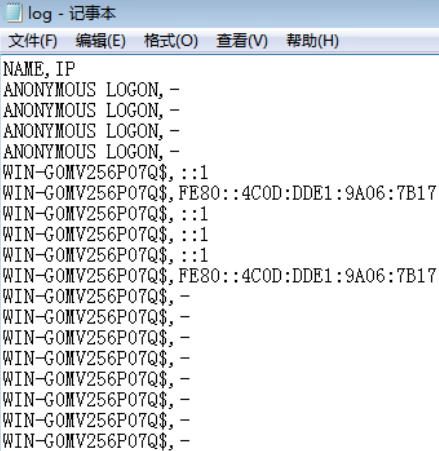


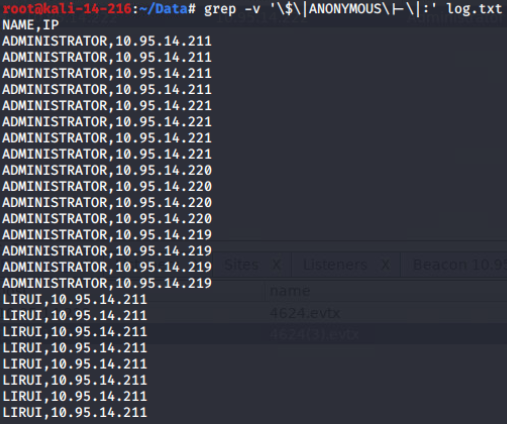




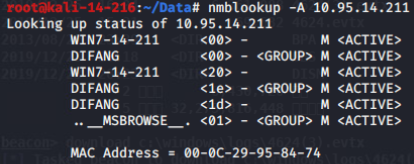














windows通过ip查主机名:

ping -a 10.95.14.211

nbtstat -A 10.95.14.211

